Pacific University
CommonKnowledge

Volume 10 (2010)

Interface: The Journal of Education, Community and Values

8-1-2010

Hacking v. Cyber War

Jeffrey Barlow
Pacific University

Hacking v. Cyber War

Hacking: The Next Generation

Posted on **April 1, 2010** by **Editor**

By Jeffrey Barlow

Recently, after suddenly needing to know much more about hacking, [1] I looked for a book from which I thought I might learn something. At the outset of this review, I should say that *Hacking: The Next Generation* is way over my head…but my purpose was to learn much more than I knew, and there are very few people out there for whom this book would not serve that same purpose. The principle author, Nitesh Dhanjani, is one of the most highly regarded and successful writers and consultants in the industry [2].

Using one of the most useful of the functions on my Kindle, I downloaded the first chapter of several highly-regarded works on Hacking, and determined that this was the one I wanted, both in terms of how well it is written and reviews found on the Web. It has not disappointed me. Scared the wits out of me, yes, but disappointed me, no.

The core audience for the book is probably best defined as I.T. professionals in charge of protecting large systems, corporations or institutions. As Dhanjani's closing remarks say:

"For any given corporation, the quest toward risk reduction and information security may seem chaotic to even the most seasoned professionals. The security team must reduce risk without getting in the way of revenue-generating business units, in addition to complying with the plethora of never-ending regulations. To bring some order to this chaos, corporations and individuals need to understand the capabilities of their adversaries. The authors sincerely hope that this book has provided you with a head start in your quest to comprehend the skill set and the mindset of attackers who are out there today."

But the nature of the book also makes it valuable for simply those wishing to be better informed on the threats of hacking. The reference to "*…The Next Generation*" in the title is to hackers who primarily use Web 2.0 functions to accomplish their intrusions. One of Dhanjani's primary arguments is that the "perimeter defense," that is, trying to block all possibly malicious intruders at the firewall, while obviously still necessary, has basically been superseded by new applications and new platforms. This is particularly true within the "cloud," virtual servers created in other

people's digital space, such as Google or Amazon's vast server aggregations.

If you intend to move operations to a cloud, as we all eventually surely will, then the authors' discussion of the distinctions between Google's approach and Amazon.Com's—the two principle providers at this time—is probably a must read for your I.T. department.

Web browsers themselves are particularly vulnerable as they need to be able to do so much for the user. Most of us have probably wondered why our particular browser is continually requesting that we download patches and updates. The answer is that intruders are discovering holes at that pace, or better, at an even faster pace as the browser builders have to become painfully aware of a vulnerability before they can fix it.

The much greater importance of social networking in Web 2.0 has also created many new opportunities and greatly leveraged the ability of hackers to "social engineer" intrusions. The authors' have many creative examples of such approaches that would probably work on just about anybody. Social networking applications such as Facebook and MySpace now give diligent intruders an opportunity to stealthily enter your "Circle of Trust."

If you already have a healthy fear of hackers and malware and have regarded the Web as the wild frontier, reading this book will take you back several eons in time, making you want to climb a convenient tree to escape the carnivores snuffling around in the dark. This is partly because the hackers themselves have, uh, evolved, to continue belaboring my Darwinian metaphor.

If previous generations were recreational hackers, or merely trying to impress teen-aged peers, today's are hard-eyed businesswomen—(In this choice of gender I am following the authors' sometimes jarring habit of reminding us that girls like to have fun, and make vast amounts of money, too.)

These frequent abrupt switches in voice are part of what makes the book so readable; the authors are continually aware of multiple audiences and segue smoothly from chatty narratives of complex intrusions to introducing the reader to the wide varieties of simple tools available on the market, or worse, for free.

For one example among dozens, want to spoof a caller ID number to prank your brother-in-law? Or perhaps to harass a former boyfriend, or to fool an executive at a major corporation into sending you the fourth quarter balance sheet on the supposition that you are one of his sales men in the field? Start at: spoofcard.com [3]. This will help you spoof your caller ID, disguise your voice, and record your call in case you want to play back some technical information or strings of numbers later. You can now do it internationally, too!

One of the most interesting elements of the book is that it shows just how easy intrusion can be. The amount of information that can be gleaned simply by using publically accessible materials is remarkable. Google caches things you would not believe, and even a simple search will often

turn up reams of financial data from major corporations, lists of credit card numbers, etc.

Want to get into somebody else's Google docs site? Go to "Stealing Documents from Online Document Stores" at Loc. 1151-1210 Kindle edition.

Do you always patch your important applications promptly? Me too! Do you always patch the old ones that you no longer use? Me either! But now I know that a hacker can use minor weaknesses in two different applications to craft one intrusion, a "blended attack." A hole in an application you don't ever use can let the intruder get into one you do use and the next thing you know, he is your daddy! Or at least you are his victim.

I suppose it is a compliment to say that the primary author thinks like a hacker, save for the fact that he is hopefully much more experienced and thoughtful than most of them. Many of the stories he tells are of exploits that he himself created as part of his work as a security consultant. Thankfully, he carefully only reveals weaknesses which have already been corrected in major software or hardware, but the sheer number of them certainly implies that there are abundant additional options out there for the criminally ambitious.

I am aware that this review must seem idiotically simple to the truly knowledgeable in this field. Fear not, the authors will challenge even you. Here is an example of one of their chapter summaries:

In this chapter, we examined the crafty and emerging attack techniques that today's new age of sophisticated attackers are employing. Whether they're conducting complex XSS attacks, turning the perimeter inside out by way of CSRF, abusing domain-based content ownership issues, or exploiting the browser software itself, attackers are evolving and learning how to poke holes into the corporate perimeter, turning it into a porous castle. As we demonstrated in this chapter, these exploits are less focused on compromising or infecting entire systems and more focused on stealing corporate secrets and data. This shift in focus allows attackers to bypass all the typical security strategies and protection mechanisms that modern software and information systems employ. Typical protection measures, such as SSL, VPNs, strong password policies, expensive firewalls, and even fully patched systems, will not stop many of these attacks. These exploits will not trigger antivirus alerts, nor will they leave an easy forensic trail for investigators to follow. In most cases, once the attacker has successfully carried out the exploit, the victim experiences no noticeable change, as the system has no persistent change to detect [4].

For the novice, the authors have previously painstakingly explained each of the above abbreviations and acronyms, or led you to an online site where even I could understand the issues. If you can't understand the above selection but would like too, the authors make that possible.

If you found the above childishly transparent, play with this one, particularly you Mac users who,

like me, probably have felt perfectly safe in our teeny market niche:

"Finding Protocol Handlers on Mac OS X: Protocol handlers on the Mac are similar to those on Windows-based machines. Various applications, including browsers, can invoke protocol handlers on the Mac. Once a protocol handler is invoked, the operating system provides a mapping between the protocol handler and the application registered with it. Any application can register a protocol handler on Mac OS X by using a program such as RCDefaultApp, or by utilizing the appropriate OS X CoreFoundation APIs. Users wishing to view all of the registered protocol handlers on their Mac OS X machine can use the following program: /* * Compile on Tiger: cc LogURLHandlers.c -o logurls -framework CoreFoundation -framework ApplicationServices or on Leopard: cc LogURLHandlers.c -o logurls -framework CoreFoundation -framework CoreServices */ #include <stdio.h> #include <AvailabilityMacros.h> #include <CoreFoundation/CoreFoundation.h> #if !defined(MAC_OS_X_VERSION_10_5) || MAC_OS_X_VERSION_MAX_ALLOWED < MAC_OS_X_VERSION_10_5 #include <ApplicationServices/ApplicationServices.h> #else #include <CoreServices/CoreServices.h> #endif /* Private Apple API... helpful for enumerating. */ extern OSStatus _LSCopySchemesAndHandlerURLs (CFArrayRef *outSchemes, CFArrayRef *outApps); static void GetBuf(CFStringRef string, char *buffer, int bufsize) { if (string == NULL) buffer[0] = '\0'; else CFStringGetCString(string, buffer, bufsize, kCFStringEncodingUTF8); } int main() { CFMutableArrayRef apps; CFMutableArrayRef schemes; int i; printf("URL Name App (Current Path)\n"); _LSCopySchemesAndHandlerURLs(&schemes, &apps); CFArraySortValues(schemes, CFArrayGetCount(schemes), *CFStringCompare, null); for (i=0; i< CFArrayGetCount(schemes); i++) { CFStringRef scheme = (CFStringRef) CFArrayGetValueAtIndex(schemes, i); CFURLRef appURL = (CFURLRef) CFArrayGetValueAtIndex(apps, i); CFStringRef appName; CFStringRef appURLString = CFURLCopyFileSystemPath(appURL, kCFURLPOSIXPathStyle); char schemeBuf[100]; char nameBuf[300]; char urlBuf[2048]; LSCopyDisplayNameForURL(appURL, &appName); GetBuf(scheme, schemeBuf, sizeof(schemeBuf)); GetBuf(appURLString, urlBuf, sizeof(urlBuf)); GetBuf(appName, nameBuf, sizeof(nameBuf)); printf("%-25s %s (%s)\n", schemeBuf, nameBuf, urlBuf); if (appURLString != NULL) CFRelease(appURLString); if (appName != NULL) CFRelease(appName); } CFRelease(apps); CFRelease(schemes); exit(0); return 0; } When the provided application is compiled and executed, it will offer output similar to that shown in Figure 4-8. Figure 4-8."

I could get really cruel, and for most readers, really boring, by reproducing some of the pages and pages of code in the book or the appendices; but I will forebear. The author takes every reader, whatever their level of ability, through every step of the exploits that he examines. If you think you are too smart to learn from this text, seek counseling, you have a problem.

One of the delights of the work, as suggest above, is that the authors are splendid teachers. Some works of this genre present the material choppily broken down into segments: horror stories, fixes, sites you should visit, annotated list of tools which are probably already outdated,

etc. This text is fully integrated, you get the information you need to know in plenty of time to take your level of understanding up a notch, and if you decide to bail off the learning curve as it rockets skyward, you still feel that you accomplished something.

The careful integration and layering of the text means that the book is highly useful for those who despair of ever walking the I.T. walk but desperately need to occasionally decipher the talk, if not actually talk it. If you should worry about the security at your operation, then you probably should read the book just to be sure that those upon whom you depend are aware of the new generations of threats.

In addition to the technical expositions, the work is also a major contribution to a fuller understanding of hacking. Dhanjani gleefully hacks hackers to show the reader how that sphere actually works. He has fascinating information on real-world examples, and again, a great deal of frightening data.

The denizens of that shadowy world are, above all, quite successful. The chances of being caught and prosecuted are miniscule. The most that we can usually hope for is to protect ourselves from becoming victims. For that reason, if you are even mildly curious, let alone if you are justifiably concerned—and we all should be—then consider reading this book.

Endnotes

[1] I had been criticized in some foreign language sources on the Web for some of my critical attitudes as expressed in my blog, which made me a bit anxious about my computer security. Once something like that happens every slowdown or weird cycle on your computer is like hearing—maybe—a floorboard creak in your house under that window you think you might have left open.

[2] Dhanjani is the author of “Network Security Tools: Writing, Hacking, and Modifying Security Tools” (O’Reilly) and “HackNotes: Linux and Unix Security” (Osborne McGraw-Hill). He is also a contributing author to “Hacking Exposed 4″ (Osborne McGraw-Hill) and “HackNotes: Network Security”. Dhanjani has been invited to talk at various information security events such as the Black Hat Briefings, RSA, Hack in the Box, Microsoft Blue Hat, and OSCON. The description is taken from his WWW site at: http://www.dhanjani.com/

[3] I am not going to follow my usual reader-friendly practice of giving formatted links in this review; I would like a running start in the event that readers want to put such information into immediate practice.

[4] Highlight Loc. 1385-93

This entry was posted in Uncategorized by **Editor**. Bookmark the **permalink [http://bcis.pacificu.edu/interface/?p=3760]** .

10 THOUGHTS ON “HACKING: THE NEXT GENERATION”

breaking news
on **January 30, 2014 at 1:56 PM** said:

I do enjoy visiting your platform, you always make me suprise with good post.

plotka
on **February 1, 2014 at 1:49 AM** said:

Incredible points. Outstanding arguments. Hold up the good spirit.

nasze miasto
on **February 1, 2014 at 3:39 AM** said:

moncler piumini

Latashia
on **February 1, 2014 at 10:36 PM** said:

I have read some good stuff here. Definitely price bookmarking for revisiting.
I wonder how a lot attempt you put to create the sort of excellent informative website.

dating online
on **February 3, 2014 at 1:49 AM** said:

Attractive section of content. I just stumbled upon your site and in accession capital to assert that I get in reality enjoyed account your blog posts. Any way I will be subscribing to your augment and even I accomplishment you access consistently rapidly.

dating
on **February 4, 2014 at 10:18 AM** said:

After examine some of the blog content on your web site now, and I incredibly like your approaches of blogging. I bookmarked it to my bookmark web site list and could possibly be checking back soon. Pls try my internet site as well and enable me know what you think.

nigeria entertainment news
on **February 4, 2014 at 10:29 AM** said:

Thanks , I've just been looking for information about this subject to your long time and yours could be the very best I've came upon so far. But, what about the conclusion? Are you particular within the supply?

nigeria entertainment news
on **February 4, 2014 at 10:39 AM** said:

I also agree with you. i believe that there are many lessons to be learned from this book. By not reading the book, we miss out on some things that are a sure impact to our life. However, I do consider you ought to be a particular maturity in order to get from this book what you need

Nigeria social network
on **February 5, 2014 at 12:16 AM** said:

great work, i adore reading your post. Maintain the excellent work.

swagbucks points generator
on **February 6, 2014 at 12:45 AM** said:

Hi to all, how is all, I think every one is getting more from this website, and your views are good in support of new users.